Not All Those Who Wander Are Lost: The Pathway towards American Data Privacy Law

Aaron Shubet

Maurice A. Deane School of Law at Hofstra University

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/hlr

Recommended Citation
Available at: https://scholarlycommons.law.hofstra.edu/hlr/vol48/iss3/12
NOTE

NOT ALL THOSE WHO WANDER ARE LOST: THE PATHWAY TOWARDS AMERICAN DATA PRIVACY LAW

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about the freedom of speech because you have nothing to say."

Edward Snowden¹

I. INTRODUCTION

Even in today's digital age of "Big Data,"² one still hopes for privacy and autonomy with regard to the use and consumption of his or her personal information, as is true with other facets of sensitive information.³ In reality, an American data subject⁴ lacks the necessary tools to prevent online actors from the collection, usage, and disclosure of most of his or her personal data within the digital marketplace.⁵ The constitutionally-founded right to privacy has long been argued, even before the turn of the twentieth century.⁶ To this day, it remains

¹ Edward Snowden (u/SuddenlySnowden), REDDIT (May 21, 2015, 2:25 PM), https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2.
² Big Data, LEXICO, https://www.lexico.com/definition/big_data (last visited May 18, 2020) (defining Big Data as "[e]xtremely large data sets that may be analysed [sic] computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions"); see Joseph A. Tomain, Online Privacy & the First Amendment: An Opt-In Approach to Data Processing, 83 U. CIN. L. REV. 1, 2-3 (2014) (describing features of the "Big Data era," including the "exponential increase in the amount and types of data collected . . . mostly without the consent of individuals whose data is being processed").
³ See Tomain, supra note 2, at 16-18. Informational privacy protects both the dignity of the data subject and his or her individual autonomy. Id. at 16; see also Parks and Recreation: The Pawnee-Eagleton Tip off Classic (NBC television broadcast Oct. 3, 2013) (quoting Ron Swanson: "People ought to have the right to be left alone.").
⁴ Council Regulation 2016/679, art. 4, § 1, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (defining data subject as one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person"). For purposes of this Note, this terminology will be adopted.
⁵ See Tomain, supra note 2, at 1, 12-14.
⁶ Samuel D. Warren & Louis D. Brandeis, Right to Privacy, 4 HARV. L. REV. 193, 193,
highly-contested because while our Constitution does not explicitly state a right to privacy, the Supreme Court has repeatedly determined that variations of the right are derived from penumbras of other rights guaranteed in the Constitution. Landmark cases that demonstrate this perceived right to privacy include Griswold v. Connecticut, Roe v. Wade, and Lawrence v. Texas, to name a few. The overarching goal connecting cases involving this implicit right to privacy is to protect an individual’s autonomy in making personal decisions about his or her body and private life without constant fear of governmental interference.

While numerous decisions have been made stating implicit findings of a right to privacy within the Constitution, one would have a difficult time finding this exact terminology. How is it then, that this right has been declared by the Court to exist, absent direct constitutional language?

Of course, a seemingly straightforward explanation would be that there can be no singular definition of privacy, thus escaping explicit constitutional capture. As “privacy” itself is somewhat of an umbrella term birthed out of societal necessity, it avoids succinct placement. When viewed from this train of thought, with the understanding that privacy is born out of societal necessity, the need for informational privacy comes clearly into focus. Just as the European Union (“EU”)

---

195 (1890).
8. 381 U.S. at 484-85 (finding that the use of contraceptives “concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees”).
9. 410 U.S. 113, 154 (1973) (concluding that the right to privacy includes qualified abortion-related decisions).
10. 539 U.S. 558, 578-79 (2003) (holding that two consenting adults engaging in homosexual activity “are entitled to respect for their private lives” and that “[t]he State cannot demean their existence or control their destiny by making their private sexual conduct a crime”).
11. See generally Beaney, supra note 7, at 214-51 (discussing the development of the right to privacy through Supreme Court cases).
15. Solove, supra note 14, at 480, 484, 486 (quoting Judith Jarvis Thompson, The Right to Privacy, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand D. Schoeman ed., 1984)) (“Perhaps the most striking thing about the right of privacy,” philosopher Judith Jarvis Thomson has observed, ‘is that nobody seems to have any very clear idea what it is.’”).
16. Solove, supra note 14, at 480, 484.
17. See id. at 484.
made data privacy to be a fundamental right, it too is necessary for the United States to adopt a more appropriate analysis of its own.\textsuperscript{18} While there truly may not be one \textit{singular} definition of privacy—as \textit{[p]rivacy is a chameleon that shifts meaning depending on context}—inaction is not an option.\textsuperscript{19} As technology advances, so too must data privacy rights.\textsuperscript{20}

This Note’s argument rests on the straightforward understanding that technological advancements have born issues which were not contemplated at the time of the Constitution’s drafting.\textsuperscript{21} In keeping up with new-world advancements, acceptance of the penumbra theory is necessary for a foundational understanding of informational privacy protections.\textsuperscript{22} For clarification purposes, \textit{Roe v. Wade} held that, although the Constitution does not explicitly provide the right to privacy, the right to personal privacy derives from the Fourteenth Amendment.\textsuperscript{23} The Fourteenth Amendment,\textsuperscript{24} in relevant part, states:

No state shall make or enforce any law which shall abridge the privileges and immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny any person within its jurisdiction the equal protection of the laws.\textsuperscript{25}

The United States’ data protection laws continue to be behind the times in comparison to other countries due to the lack of comprehensive data privacy regulation.\textsuperscript{26} The EU, for example, enacted the General Data Protection Regulation ("GDPR") as of April 2016, which aims to give

\begin{footnotesize}
\begin{enumerate}
    
    
    \item Jerry Kang, \textit{Information Privacy in Cyberspace Transactions}, 50 STAN. L. REV. 1193, 1202 (1998); \textit{see infra Part IV} (proposing a comprehensive data privacy framework).
    
    
    \item See Warren & Brandeis, \textit{supra} note 6, at 195 ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‘to be let alone.’") (internal citation omitted).
    
    \item See generally Jolly, \textit{supra} note 14 (identifying various industries with data privacy regulations and the varying degrees thereof).
    
    \item Roe v. Wade, 410 U.S. 113, 132 (1973). Noting that:
        In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment . . . ; in the Four and Fifth Amendments . . . ; in the penumbras of the Bill of Rights, \textit{Griswold v. Connecticut}, 381 U.S., 484-485; in the Ninth Amendment . . . ; or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment, see \textit{Meyer v. Nebraska}, 262 U.S. 390, 399 (1923). These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty," \textit{Palko v. Connecticut}, 302 U.S. 319, 324-25 (1937), are included in this guarantee of personal privacy.
        \textit{Id.}
    
    \item U.S. CONST. amend. XIV, § 1.
    
    \item \textit{Id.}
    
    \item Linn, \textit{supra} note 13, at 1316.
\end{enumerate}
\end{footnotesize}
fundamental control to EU citizens and residents over their personal data.27 Comparatively, forced to rely on a myriad of piecemeal legislation, an American data subject is left with an inefficient and insecure federal framework for data privacy.28 Currently, some sectoral laws have been adopted while other areas are left up to self-regulation.29 Consequently and unsurprisingly, public distrust in this self-regulatory regime continues to rise, ultimately stemming from the insurmountable pitfalls of the current piecemeal privacy patchwork.30

Part II of this Note begins by examining the various ineffective U.S. data privacy frameworks involving sectoral lawmaking and the preferred method of self-regulation as “best practices.”31 The United States’ sentiment towards privacy is then juxtaposed with that of the EU’s, which elevates data privacy to fundamental right status.32 Part II continues by discussing America’s constitutional underpinnings for the right to privacy and takes a look at the technology industry’s opinion on the matter.33 Part II concludes with an examination of standard privacy notice practices and determines whether “idealized consent” is accurately dubbed as “legal fiction” or is something entirely obtainable.34 Part III looks at the developing landscape of federal data privacy law by giving a side-by-side analysis of Senator Ron Wyden’s bill, Intel’s proposal, and the California Consumer Privacy Act of 2018 (“CCPA”), and further displays why these models are insufficient to tackle present issues.35 Lastly, Part IV proposes a framework for federal legislation and outlines the individual rights to be enshrined therein.36

II. THE TRANSATLANTIC DIVIDE: DIFFERING SENTIMENTS TOWARDS DATA PRIVACY

To better grasp the current state of data privacy, it is first worth mentioning the difference between “cybersecurity” and “data security.”37 Most of the time, cybersecurity is used interchangeably with data

27. GDPR, supra note 4, at arts. 1, 99 (declaring the fundamental right to protection of personal data and identifying the effective date of May 25, 2018, respectively).
28. Linn, supra note 13, at 1316.
29. Id.
31. See infra Part II.A.
32. See infra Part II.B.
33. See infra Parts II.C–D.
34. See infra Part II.E.
35. See infra Part III.
36. See infra Part IV.
security.\textsuperscript{38} However, cybersecurity is much broader than data security, as it encapsulates both network and system security measures.\textsuperscript{39}Cybersecurity law “promotes not only (1) confidentiality but also (2) integrity and (3) availability (known in cybersecurity circles as the ‘CIA Triad’).”\textsuperscript{40} References to data protection have become “particularly prominent” following the GDPR’s enactment.\textsuperscript{41} Data protection law closely relates to cybersecurity law as it also requires companies to adopt procedural safeguards and holds them accountable for data breaches.\textsuperscript{42} This Note focuses on data protection as it relates to the average American data subject’s expectation of informational privacy.\textsuperscript{43} While this Note’s argument revolves around informational privacy, the legislative end is inextricably tied to cybersecurity concerns, and, as such, certain provisions relating strictly to cybersecurity are included.\textsuperscript{44}

The current rate that international data trades at and the speed at which personal information may flow to bridge the transatlantic space continues to cause worry among American technology firms.\textsuperscript{45} Significant uncertainties surround international data transfer as legal bodies clash and the stakes have become such that failure to enact comprehensive legislation is at an all-time high.\textsuperscript{46} A study conducted in March of 2016 by the U.S. Department of Commerce found that “$260 billion in digital services trade moves between the United States and the EU annually.”\textsuperscript{47} To draw comparisons to the reigning principals driving privacy law, Nikolaus Peifer, Director of the Institute for Media Law and Communications Law at the University of Cologne, explains that “[e]ncryption is based to some extent on the idea that the law won’t protect your rights, so you have to protect yourself . . . The European tradition is that the law will protect you.”\textsuperscript{48}

Whereas the EU views data privacy law as a reflection of the fundamental rights of its citizenry, the United States’ informational privacy law is founded within the marketplace.\textsuperscript{49} This type of bilateral

\textsuperscript{38} Id.
\textsuperscript{39} Id.
\textsuperscript{40} Id.
\textsuperscript{41} Id. at 170-71.
\textsuperscript{42} Id. at 171.
\textsuperscript{43} See infra Parts II.C, II.E, IV.
\textsuperscript{44} See infra Part IV.
\textsuperscript{46} See id.
\textsuperscript{48} Levine, supra note 45.
\textsuperscript{49} Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 GEO. L.J. 115, 132 (2017) (“Unlike the EU’s data subject, U.S. law does not equip the privacy consumer
self-interest driven marketplace scheme places emphasis on personal information commoditization and leaves U.S. lawmaking to follow the doctrines of fairness.  

50  This can be further evidenced by a quick observation of the language used in data privacy related statutes.  

As a matter of fact, U.S. privacy statutes place the individual immediately within marketplace relations through the use of such statutory language as “consumer, customer, or ‘subscriber’ of telecommunications.”  

51

The presumptive permissibility of the free flow of information and the subsequent processing of any personal data is a widely accepted principle in the U.S., unless laws otherwise limit its application.  

52

Insufficient data protection continues on through a hodgepodge statutory regime, both at the state and federal levels, with the main drawback being the necessary presence of a “horror story” to further shock growth into existence.  

53 This is best exhibited by the historic tendency of swift legislative data privacy action only after demonstrations of extreme, abusive data practices.  

Beginning with a national inspection, Subpart A explores the fragmented sectoral data privacy regime throughout the United States.  

54 Subpart B then discusses the EU’s GDPR and its global implications.  

55 Subpart C discusses the various implicit constitutional findings of the right to privacy and congressional regulatory authority on the matter.  

56 Subpart D examines the various viewpoints of those in the tech industry: Subpart D.1 finds fault in the tech giants’ call for reformed governmental surveillance,  

57 Subpart D.2 focuses on Facebook’s privacy violations as being the quintessential rallying cry for the need of legislative change,  

58 and Subpart D.3 calls attention to Tim Cook’s address at the Fortieth International Conference of Data Protection and Privacy Commissioners.  

59 Lastly, Subpart E tackles the issue of whether idealized consent is truly legal fiction or an obtainable reality.  

50 Id. (“Personal information is another commodity in the market, and human flourishing is furthered to the extent that the individual can maximize her preferences regarding data trades.”).  

51 See id.  

52 Id.  

53 Id. at 135.  

54 Id. at 136.  


56 See infra Part II.A.  

57 See infra Part II.B.  

58 See infra Part II.C.  

59 See infra Part II.D.1.  

60 See infra Part II.D.2.  

61 See infra Part II.D.3.  

62 See infra Part II.E.
A. Shortcomings of Sectoral and Piecemeal Lawmaking

The United States, failing to adopt an all-encompassing rights-based federal data privacy law like that of the EU, has chosen to rely on a system of “industry norms, codes of conduct and the consumer marketplace to protect personal privacy.” This is due, in part, to the varying views and sentiments towards the right to privacy existing between the two entities. The EU understands data privacy to be a fundamental human right, protecting individuals from unfair corporate data collection. The United States, in contrast, follows a more fragmented approach to data privacy regulation—passing laws across specific target areas, while leaving the rest up to self-regulation. These optional guidelines and frameworks created by governmental agencies can often “overlap, dovetail, and contradict one another” due to the disjointed nature of the coverage and the general preference for self-regulation to be considered “best practices.”

In an attempt to protect certain sensitive personal information, narrowly-carved, federal privacy-related laws and regulations safeguard the collection and use of particular categories of information, such as financial information, health information, and electronic communications. Examples of federal privacy laws include: the Federal Trade Commission Act, the Fair Credit Reporting Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Children’s Online Privacy Protection Rule.

---

64. Linn, supra note 13, at 1315-18.
68. Id.
70. 15 U.S.C. § 1681 (2018) (governing the collection and use of certain financial information, such as consumers’ credit worthiness, credit standing, credit capacity and general capacity used in determining credit eligibility).
Understanding the general operating principles of the Federal Trade Commission ("FTC")—revolving around a responsive nature rather than a preventative one—reveals that the federal regulations in place for data privacy do not address the fundamental underlying issue: "unjustified, mass data collection itself."74 At the state level, "[a]ll 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands" have some varying form of breach notification law involving personally identifiable information.75 As a result of not having one single comprehensive federal law, the United States has hundreds of data privacy laws across the country.76 California alone has twenty-five state privacy laws, including the CCPA.77 According to Cheryl Wang, writing for the Columbia Undergraduate Law Review, "it is precisely this dispersive and disorganized nature of different states' regulations that creates a highly inefficient and undefined system for protecting privacy" throughout the United States.78 With no two states having the same informational privacy and security laws,79 the current regulatory framework lacks the broad accountability necessary to provide companies with the requisite incentives to protect consumer data.80

In February of 2019, 121 data brokers81 that collect and sell data about Vermont residents registered with the Vermont Secretary of State following the enactment of the country's first law governing the data broker industry.82 Vermont attempted to bring this industry—shrouded in


77. Id.

78. Wang, supra note 74.


80. Wang, supra note 74.

81. 9 VT. STAT. ANN. tit. 9, § 2430(4)(A) (West 2019). A data broker is a "business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." Id. There are three types of data brokers:

(1) There are people search sites, where users can input a piece of data, such as a name... and get personal information on that person either for free or for a small fee... [(2)] There are data brokers that focus on marketing... They develop... on individuals which can be used to tailor marketing... [(3)] Lastly, there are data brokers such as ID Analytics that offer risk mitigation products to verify identities and help detect fraud.

82. Steven Melendez, A Landmark Vermont Law Nudges over 120 Data Brokers out of the

secrecy—out into the sunlight; the ultimate “goal was to give residents one public database where they can find clear information about all companies that sell their data . . . .” Data is equivalent to power in today’s “digital economy,” as “[m]ulti-national corporations have made farming data from monitoring everything we do—what we buy, who we talk to, where we take vacation—a core business strategy.”

In May of 2014, after it conducted an in-depth study on nine individual data brokers, the FTC released its 110-page report. The report lists several recommendations, including: “legislation requiring consumer-facing entities to disclose that they share data with brokers, and allow them to opt out,” and a call for “data brokers to create a centralized mechanism, such as a portal, to provide consumers access to their data . . . .” Unfortunately, Congress has yet to follow through on the problem of data privacy. The FTC’s report—calling for transparency, opt-out mechanisms, and informative consumer tools—is directly in line with this Note’s proposed solution: comprehensive federal data privacy regulation.

B. What Is the GDPR Exactly?

The EU’s GDPR was formally adopted in 2016 and officially went into effect on May 25, 2018. The aim of the GDPR is to lay down rules relating to data protection with regard to the processing of personal data. This regulation finds power of enforcement through the protection of

---


83. See Douglas MacMillan, Data Brokers Are Selling Your Secrets. How States Are Trying to Stop Them., WASH. POST (June 24, 2019, 5:54 PM), https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them ("Until recently, Randy Koloski had never heard of Amerilist, a small business 25 miles north of Manhattan. But for $150, Amerilist makes available a list of information on 5,000 people that includes Koloski’s name, home address, age, religion, education level and income.").


86. Id. at 49-54; Grauer, supra note 81.

87. Grauer, supra note 81.

88. See infra Part IV.

89. GDPR, supra note 4, at art. 99(2).

90. Id. at rec. 2.
fundamental rights and freedoms of natural persons and the free movement of such personal information.\textsuperscript{91} Differing from the United States’ market-based theory, an EU data subject enjoys near full control and ownership as personal data privacy is a fundamental right guaranteed by the European Union Charter of Fundamental Rights.\textsuperscript{92} For purposes of this Note’s objective, the topic of consent\textsuperscript{93} shall be discussed in further detail in Part III as it pertains to U.S. law.\textsuperscript{94}

Since the GDPR’s enactment, data subjects globally have noticed a bombardment of consent notifications immediately upon arrival onto a new website pertaining to the website’s respective cookie policies, regardless of the geographic location of the operating individual.\textsuperscript{95} This seemingly-innocuous interruption of web usage is thanks to the global implications of the GDPR.\textsuperscript{96} Article 7 of the GDPR lays out the conditions for consent, stating that “\textquote{[w]here processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.\textquote{}}”\textsuperscript{97} The Article 7 provisions work together to create the GDPR’s consent regime: An individual must give clear and affirmative consent to the use of their data in the purported manner.\textsuperscript{98}

\textquote{“Cookie” is the term given to a packet of data that is sent from a website to a user’s computer and then sent back to the website “without changing or altering it.”\textquote{}}\textsuperscript{99} The purposes of website cookies can vary, but they boil down to tailoring a website to fit a particular consumer’s needs and personal interests.\textsuperscript{100} For example, a retailer may use cookies to keep

\begin{footnotesize}
91.\textsuperscript{ } Id. at rec. 2–3.
92.\textsuperscript{ } Charter of the Fundamental Rights of the European Union, art. 8, Oct. 26, 2012, 2012 O.J. (C 364) 391 (\textquote{1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.\textquote{}}).
93.\textsuperscript{ } GDPR, supra note 4, at art. 7.
94.\textsuperscript{ } See infra Part III.
96.\textsuperscript{ } GDPR, supra note 4, at art. 7(1); see Schofield, supra note 95.
97.\textsuperscript{ } GDPR, supra note 4, at art. 7(1); id. at art. 4(2) (\textquote{\textquotenoquotesingle Processing\textquotenoquotesingle means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation [sic], structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.\textquotenoquotesingle id. at art. 4(7) (\textquote{\textquotenoquotesingle Controller\textquotenoquotesingle means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data . . . .\textquotenoquotesingle)) For the purposes of this Note, this terminology will be adopted.
98.\textsuperscript{ } Id. at art. 7.
100.\textsuperscript{ } What Are Cookies?, WEBWISE (Oct. 10, 2012), http://www.bbc.co.uk/webwise/guides/abo
\end{footnotesize}
track of items in a consumer’s “shopping cart.”\textsuperscript{101} Without the website and the computer recognizing each other in this fashion, online shopping would not be possible.\textsuperscript{102}

So then how is it that cookies relate to the GDPR?\textsuperscript{103} Simply put, a cookie can be used to uniquely identify an individual; thus classifying it as personal data and bringing it within the purview of the GDPR.\textsuperscript{104} It is important to remember that all of this is done in an effort to remain compliant with the GDPR’s consent obligations\textsuperscript{105}—which require data processors to gain clear, unequivocal acceptance and consent to cookie usage, in addition to providing opt-out capabilities to those that have previously given consent.\textsuperscript{106}

Additionally, not only does the GDPR place the initial decision in the hands of the EU data subject, but it also gives him or her a few avenues of recourse when it comes to incorrect or irrelevant information.\textsuperscript{107} An EU citizen seeking to correct misinformation may exercise his or her Article 16 Right to Rectification, which states that “[t]he data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.”\textsuperscript{108} Alternatively, the EU citizen wishing for the deletion of irrelevant collected information can exercise his or her Article 17 Right to Erasure, which states that “[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one” of any of the provided for situations occur.\textsuperscript{109}

\textsuperscript{101} What Are Cookies?, supra note 99.
\textsuperscript{102} Id. (“Without cookies,” a consumer’s shopping cart “would reset to zero every time you clicked a new link on the site.”).
\textsuperscript{103} Laura Vegh, Cookies Consent Under the GDPR, EU GDPR COMPLIANT (Feb. 14, 2018), https://eugdprcompliant.com/cookies-consent-gdpr; see Schofield, supra note 95; see also GDPR, supra note 4, at rec. 30 (“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocols address, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”) (emphasis added).
\textsuperscript{104} See Vegh, supra note 103.
\textsuperscript{105} See GDPR, supra note 4, at art. 7(2).
\textsuperscript{106} GDPR, supra note 4, at arts. 7(2)–(3); see GDPR, supra note 4, at art. 21 (“[Article 21(1):] The data subject shall have the right to object, on grounds relating to his or her particular situation . . . . [Article 21(2):] Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.”).
\textsuperscript{107} See infra text accompanying notes 108-09.
\textsuperscript{108} GDPR, supra note 4, at art. 16.
\textsuperscript{109} Id. at art. 17 (listing the following scenarios where a data subject may exercise her right to erasure: (1) the personal data is no longer necessary in relation to the original collection purpose, (2) the data subject withdraws consent, (3) the data subject objects pursuant to Article 21(1) or Article 21(2), (4) the personal data has been unlawfully processed, (5) the personal data must be erased for
C. The Constitutional Foundation for Congressional Action

The right to privacy, originally dubbed the “right to be let alone,” has been broadened to encompass things of both intangible and tangible nature as the progression of society—in ways of political, social, and economic change—has enticed the need for such expansions. Just as technological advancements shape society, they also alter our understanding of constitutional liberties. Seminal cases like *Meyer v. Nebraska*, *Pierce v. Society of Sisters*, *Griswold v. Connecticut*, *Planned Parenthood v. Casey*, and *Obergefell v. Hodges* have all been pivotal in the shaping and recognition of societal expectations of privacy. The argument for an implicit right to privacy is further bolstered when individual amendments are examined, not as restrictions on the government, but as protections given to the individual.

__Compliance with a legal obligation, and (6) the personal data has been collected in relation to the offer of information society services. Opponents of an American right to be forgotten fear that it would come at the cost of First Amendment liberties, such as free speech. Hillary C. Webb, Note, “People Don’t Forget”: The Necessity of Legislative Guidance in Implementing a U.S. Right to Be Forgotten, 85 GEO. WASH. L. REV. 1304, 1309 (2017). However, it need not be so black and white as Viviane Reding, Vice President of the European Commission, stated that “[t]he right to be forgotten is of course not an absolute right . . . . Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media.” Viviane Reding, Vice President, European Comm’n, EU Justice Comm’r, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012) (transcript available at http://europ.eu/rapid/press-release_SPEECH-12-26_en.htm). The constitutionality of the right to rectification and the right to erasure go beyond the scope of this Note, but their mention is relevant due to California’s adoption of the right to erasure, albeit limited, in the California Consumer Privacy Act of 2018. See infra Part III.C.

110. Warren & Brandeis, supra note 6, at 193 (“Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term ‘property’ has grown to comprise every form of possession —intangible, as well as tangible.”).

111. See Tim Sharp, Right to Privacy: Constitutional Rights & Privacy Laws, LIVE SCI. (June 12, 2013), https://www.livescience.com/37398-right-to-privacy.html (stating that “the boundaries of personal privacy” have changed “largely due to social media and an atmosphere of ‘sharing’”).

112. 262 U.S. 390, 400-01 (1923) (concluding that education and the acquisition of knowledge are matters of utmost importance, the determination of which is within parental privacy).

113. 268 U.S. 510, 534-35 (1925) (protecting the fundamental right of a parent to control the upbringing and education of a child under his or her control).

114. 381 U.S. 479, 480, 484-86 (1965) (finding that the intimate choice between husband and wife to use contraception lies within the zone of privacy emanating from the penumbras of the Bill of Rights).

115. 505 U.S. 833, 846-48 (1992) (reaffirming a woman’s constitutional right to terminate her pregnancy, founded within the “substantive liberties protected by” the Due Process Clause of the Fourteenth Amendment).

116. 133 S. Ct. 2584, 2604-05, 2607-08 (2015) (extending the holding of Lawrence v. Texas, which held in favor of an implicit right to privacy between two consenting homosexual adults, to the conclusion that the fundamental right to marry is guaranteed to same-sex couples by the Equal Protection and Due Process Clauses of the Fourteenth Amendment).

117. See Sharp, supra note 111 (recognizing that Griswold v. Connecticut was the first case to create a zone of privacy).

118. See id. (listing the individual protections afforded by the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments).
To clarify this idea of negative liberties, a plain reading of the First Amendment reveals that it protects the privacy of one’s beliefs, but this is through the negative lens prohibiting the government from establishing a national religion or impeding on the free exercise thereof.\(^{119}\) In the same fashion, the Third Amendment “protects the privacy of the home against the use of it for housing soldiers” through the governmental restriction on quartering soldiers in private homes without the owner’s consent.\(^{120}\) The Fourth Amendment protects the privacy of one’s self through the restriction against unjustifiable governmental searches and seizures.\(^{121}\) The Fifth Amendment grants the right against self-incrimination, thus limiting governmental authority over the compulsion of private or personal information.\(^{122}\) Additionally, the Ninth Amendment has been construed as validation that the Bill of Rights should not be read as an exhaustive list of privacy protections.\(^{123}\) Equally important, the Fourteenth Amendment, with the power of the Due Process Clause, has been understood as protecting all rights previously discussed while being fully attributable to the states.\(^{124}\)

The Supreme Court, in *Reno v. Condo*, squarely upheld Congress’ constitutional authority to regulate, at least to a certain extent, privacy under the Commerce Clause.\(^{125}\) Article I, Section 8, Clause 3 of the U.S. Constitution, otherwise referred to as the Commerce Clause, grants Congress the authority to regulate channels of commerce among the states, with foreign nations, and with the Indian Tribes.\(^{126}\) Congress is authorized to regulate the “channels of interstate commerce; instrumentalities, peoples, and things used in interstate commerce; and other activities substantially related to interstate commerce.”\(^{127}\) Recalling the rate at which data trades internationally, Townsend Feehand, Chief Executive of IAB Europe, commented that “[i]nternational data transfers are the lifeblood of the digital economy.”\(^{128}\)

---

119. U.S. CONST. amend. I.
120. Id. amend. III; Sharp, *supra* note 111.
121. U.S. CONST. amend. IV; Sharp, *supra* note 111.
123. U.S. CONST. amend. IX; Sharp, *supra* note 111.
This is where another distinction must be made between cybersecurity and data privacy. Critics of federal cybersecurity legislation argue that an expansive view of the Commerce Clause, as it applies to regulating the free flow of information, would exceed the Framers’ intended scope. In reality, even when interpreted narrowly, the Commerce Clause covers cybersecurity as most data are stored on cloud services, all of which may have zero connection to a physical location. From this it follows that securing said data, even when performed without commercial motive, falls within the scope of the Commerce Clause. This understanding rests on the interwoven nature of cybersecurity and data privacy, and the role that this data would nonetheless ultimately play on interstate commerce. The procedural safeguards that cybersecurity—and data protection in particular—would require inevitably impact the commercial flow of information; because cybersecurity is inextricably tied to data protection, procedural safeguards of the former are substantially related to the ultimate desire for the latter. It is for this reason that “[r]egulating how companies secure and protect this valuable commodity [would] inevitably regulate how the data flows across state lines.” As the judiciary has recognized, there can be little doubt that “[a]s both the means to engage in commerce and the method by which transactions occur, ‘the internet is an instrumentality and channel of interstate commerce.’” With this understanding, “regulation of the Internet [thus] impels traditional Commerce Clause considerations.”

Thanks to the pervasiveness of the Internet and the “gestation of the ‘always online’ society,” the scale of data farming has risen exponentially without regard to global borders. Not only does precedent suggest the constitutional underpinning for an argument in favor of a right to data privacy through the Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, but the rate at which data trades, both interstate and internationally, also suggests congressional authority by means of Commerce Clause regulation.

129. See supra Part II (explaining that cybersecurity is a broader concept than data security).
130. U.S. CONST. art. I, § 8, cl. 3; Kosseff, supra note 37, at 179-80.
131. Kosseff, supra note 37, at 180-81.
132. U.S. CONST. art. I, § 8, cl. 3; Kosseff, supra note 37, at 180-81.
133. See Kosseff, supra note 37, at 179, 180-81.
134. Id.
135. Id. at 181.
136. United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).
137. Am. Libraries Ass’n v. Pataki, 969 F. Supp. 160, 173 (S.D.N.Y. 1997) (“The Internet is more than a means of communication; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos.”) (emphasis added).
138. Marr, supra note 84.
139. U.S. CONST. art. I, § 8, cl. 3; id. amends. III, IV, V, IX, XIV; Pritzker & Ansip, supra note 47 (noting that the trade of goods and services between the United States and Europe totals $2.7
D. Tech Giants and Data Privacy: Wanting to Have Their Cake and Eat It Too

The growth of technology and the ease at which the digital environment may be accessed “presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure.” Of course, certain governmental agencies have made strides in ways of protecting certain sensitive information, but a greater degree of data security is necessary. Should an all-encompassing rights-based data privacy regime take force, consumers can attain a greater sense of confidence as to where their data is going and what it is being used for.

1. Tech Giants’ Acknowledgement of Privacy Rights

On December 9, 2013, tech giants Google, Facebook, Microsoft, Apple, Yahoo, AOL, LinkedIn, and Twitter published an open letter calling to reform global surveillance practices in light of the then recent NSA leaks. In addition to the open letter, the companies collectively listed five principles (with a sixth principle added later) for governments to adhere to while conducting surveillance. While these principles were strictly directed towards governmental surveillance, this Note argues that they should be equally applicable to private actors because to do otherwise would go against the main objective: protecting privacy interests against powerful actors, regardless of whether they are private or public.

The first principle is “Limiting Governments’ Authority to Collect Users’ Information.” Here, the tech giants call for limiting surveillance for specific reasons and only for lawful purposes and advise against government pursuit of bulk data collection. This principle aims to

---

141. See Jolly, supra note 14 for a discussion on various federal and state laws addressing U.S. data protection.
142. See generally GDPR, supra note 4, at art. 7 (stating the necessary underlying principle of unambiguous, affirmative consent to data collection and processing practices).
145. Tomain, supra note 2, at 18, 19.
146. Putting Principles into Action, supra note 144.
147. Id.
safeguard the trust founded within the Internet by protecting individual privacy rights, the likes of which are violated if consent is not first freely given.\textsuperscript{148} However, it is irrelevant whether it is a public or private data collector;\textsuperscript{149} rather, what is important are the privacy concerns individuals have in understanding the scope and purpose of data collection and processing in correlation to the consent provided.\textsuperscript{150}

The second principle is “Oversight and Accountability.”\textsuperscript{151} This principle would require a clear and comprehensible statutory framework to provide unequivocal notice to processors about the scope of a government’s ability to “collect or compel the production of information.”\textsuperscript{152} Similarly, the third principle, “Transparency About Government Demands,” notes that transparency is of utmost importance in determining the permissible power and scope of surveillance programs.\textsuperscript{153} An opt-in regulatory regime, the necessity of which is discussed in Part IV of this Note, applied to both the private and public sector would safeguard against privacy infringement by providing material information about an institution’s data practices.\textsuperscript{154}

The fourth principle, “Respecting the Free Flow of Information,” was included in light of the then newly-imposed GDPR.\textsuperscript{155} This principle states that the free flow of data is essential to today’s digital economy and governments should not only permit, but also promote, the free flow thereof.\textsuperscript{156} Here, the tech giants maintain that private actors should not be subject to the same restrictions as the government.\textsuperscript{157} However, it is not the nature of the entity that matters—whether it be private or public—rather, what matters are the data subject’s privacy interests in being free of mass data collection and the subsequent creation of detailed data profiles without user consent.\textsuperscript{158}

Within the fifth principle, “Avoiding Conflicts Among Governments,” the reform calls on governments to propose a robust, all-encompassing international privacy regime to better protect a corporation from conflicting laws.\textsuperscript{159} Lastly, the sixth principle, “Ensuring Security

\textsuperscript{148} Id.; see Tomain, supra note 2, at 19.

\textsuperscript{149} Neil M. Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934, 1935 (2013) (“Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers.”); Tomain, supra note 2, at 19.

\textsuperscript{150} See Richards, supra note 149, at 1935; Tomain, supra note 2, at 19.

\textsuperscript{151} Putting Principles into Action, supra note 144.

\textsuperscript{152} Id.

\textsuperscript{153} Id.

\textsuperscript{154} Tomain, supra note 2, at 19; see infra Part IV.

\textsuperscript{155} Tomain, supra note 2, at 19; Putting Principles into Action, supra note 144.

\textsuperscript{156} Putting Principles into Action, supra note 144.

\textsuperscript{157} Tomain, supra note 2, at 19-20; see Putting Principles into Action, supra note 144.

\textsuperscript{158} Tomain, supra note 2, at 19-20; see Putting Principles into Action, supra note 144.

\textsuperscript{159} Putting Principles into Action, supra note 144.
and Privacy Through Strong Encryption,” calls for improved encryption across the board to guard individuals, corporations, and governments against breaches. While all six principles were directed against governmental intrusion, the argument fails as it ignores the interwoven relationship between the private and public spheres: “[T]hey use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide.”

2. Facebook Under Strict Governmental Scrutiny

Whether a corporation chooses the opt-out or opt-in model of consent, the FTC retains enforcement capabilities through general consumer protection laws prohibiting “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.” Currently, the only guidance pertaining to obligations in respect to disclosures of personal information follows an opt-out regime, holding that a financial institution may not disclose categorized personal information to a nonaffiliated third party unless: (1) such disclosure has been made to the data subject, (2) the consumer has been given an opportunity to object, and (3) the consumer has been apprised of her right to exercise nondisclosure.

In November of 2011, Facebook settled a claim brought by the FTC asserting Facebook had deceived consumers through its terms and conditions agreement in promising that its users’ information would be kept private. Instead, this information was shareable and made public. The FTC’s eight-count complaint against Facebook was an attempt to ensure Facebook’s privacy policies aligned with the promises made to its consumers. Most importantly, Facebook was required to

160. Id.
161. Richards, supra note 149, at 1958; see Tomain, supra note 2, at 19–20.
162. See Fed. TRADE COMM’N, supra note 66, at 15-16.
165. Id. § 6802(b)(1)(A).
166. Id. § 6802(b)(1)(B).
167. Id. § 6802(b)(1)(C).
169. Id.
170. Id. The FTC complaint identified the following instances where Facebook’s actions did not line up with privacy promises made: (1) Facebook ensured certain information, such as friends lists, would remain private but this information was instead public without consumer notification; (2) users were assured third-party applications installed would only have access to relevant information, but instead, third parties could access almost all personal information; (3) users were assured they could restrict sharing by changing their privacy settings to “friends only,” but their data was still shared with third-party applications; (4) Facebook did not certify the security of third-party applications as claimed; (5) Facebook shared personal information with advertisers, which it promised it would not
take several steps to ensure promised data privacy and protection, “including giving consumers clear and prominent notice and obtaining consumers’ express consent before their information is shared beyond the privacy settings they have established.”171 The FTC can intervene and require an opt-in consent model if it’s deemed necessary to prevent further deceptive business practices, as seen here.172 Public concern continued to grow following Facebook’s March 16, 2018, statement regarding its data breach, leaving an estimated 87 million users exposed to Cambridge Analytica.173

The March statement declared that Aleksandr Kogan created an application called “thisisyourdigitallife,” which asked users to give consent to and login with their Facebook credentials in order to utilize its personality prediction features.174 Paul Grewal, Vice President & Deputy General Counsel of Facebook, stated that “[a]lthough Kogan gained access to [users’ private information] in a legitimate way and through the proper channels that governed all developers on Facebook at that time, he did not subsequently abide by our rules. By passing information on to a third party... he violated our platform policies.”175 Data privacy concerns then led to a Senate hearing in April of 2018, where senators of the House Energy and Commerce Committee called into question the current atmosphere of data privacy and the possible need to regulate Facebook with governmental oversight.176 Ed Markey, a Democratic Senator from Massachusetts, stated that “[t]he day of reckoning for American privacy has arrived... Facebook now has to deal with how much people understand about how vulnerable all their information is and how few protections are on the books. So I do think this is a legislating moment.”177

---

171. Id.
172. Id.
173. See Sherr, supra note 30.
174. Id.
177. Id.; see also Mike Isaac & Sheera Frenkel, Facebook’s Woes Rise as Hackers Expose Data of 50 Million Users, N.Y. TIMES, Sept. 29, 2018, at A18 (“Breaches don’t just violate our privacy. They create enormous risks for our economy and national security,’ Rohit Chopra, a commissioner of the Federal Trade Commission, said in a statement. ‘The cost of inaction is growing, and we need answers.’”); Louise Matsakis & Issie Lapowsky, Everything We Know About Facebook’s Massive Security Breach, WIRED (Sept. 28, 2018, 3:03 PM), https://www.wired.com/story/facebook-security-breach-50-million-accounts (discussing a later Facebook security breach that may have affected 90 million users).
Routinely becoming the bearer of bad news, Facebook’s privacy integrity has further proven insufficient as the social network disclosed on September 28, 2018, that an unprecedented security breach had impacted nearly 50 million users, with an additional 40 million users considered to be at risk. Facebook continues to be a prime example of the need for congressional action in ways of data protection and security. Uniquely, this breach differs from the Cambridge Analytica incident in that Cambridge Analytica used a then legitimate application to access and siphon data from Facebook users after affirmative consent, while the more recent breach actually allowed hackers to illegitimately take full control of impacted accounts. Mark R. Warner, a Democratic Senator from Virginia, commented on this breach as being yet another “sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users.”

3. Cook Praises the GDPR

At the Fortieth International Conference of Data Protection and Privacy Commissioners on October 24, 2018, Tim Cook gave an impassioned speech praising the EU in ways of individual data privacy protection. It was with admiration for the EU in mind that he called for similar rights to be enshrined by U.S. legislation. Cook asserted that “[t]echnology’s potential is, and always must be, rooted in the faith people have in it,” and pointed out that at the current rate of data misuse, public trust, and in turn, technological advancement will falter.

Cook called for the world to follow the EU’s lead—with its enactment of the GDPR—to create a similar all-encompassing rights-
based data privacy law in the United States.\textsuperscript{187} With the support of Apple behind him, the comprehensive federal legislation he calls for would be founded upon the following four principles: (1) data minimization (companies should either de-identify consumer data or not collect it at all),\textsuperscript{188} (2) consumers should always have the right to know what data is being collected, to what extent, and for what purpose;\textsuperscript{189} (3) the data subject’s right to access their personal data stored with the collector should be respected,\textsuperscript{190} and (4) everyone has a right to security of their data.\textsuperscript{191} This so-called “right to security,” as Cook puts it, is a clear acknowledgment that proper data privacy legislation cannot come about without accompanying data security provisions.\textsuperscript{192} Data privacy law requires cybersecurity standards capable of providing American data subjects with the proper tools necessary to hold covered entities accountable for data security failures.\textsuperscript{193}

Following Cook’s speech, Acxiom, one of the nation’s leading data brokerages, offered support for the call for federal legislation.\textsuperscript{194} Acxiom—which originally opposed the previously mentioned Vermont law on data brokers—took the time to clarify its distaste: “What everyone must understand is that the cost of compliance for all businesses in the US will be punitive and detrimental to our economy if everyone must adhere to multiple and independent state laws versus a singular, united set of


\textsuperscript{188} Tim Cook (@tim_cook), TWITTER (Oct. 24, 2018, 5:57 AM), https://twitter.com/tim_cook/status/1055035541996089344.

\textsuperscript{189} Tim Cook (@tim_cook), TWITTER (Oct. 24, 2018, 5:57 AM), https://twitter.com/tim_cook/status/1055035543933849600.

\textsuperscript{190} Tim Cook (@tim_cook), TWITTER (Oct. 24, 2018, 5:57 AM), https://twitter.com/tim_cook/status/105503554244911105. Here Cook advocates for the individual data subject’s right to correct and delete personal data collected. \textit{Id}. As previously discussed, the Right to Rectification and Right to Erasure go beyond the scope of this Note’s proposed solution. \textit{See infra} Part IV. However, the mention of which is noteworthy as it indicates industry willingness. \textit{See} Tim Cook (@tim_cook), \textit{supra}.

\textsuperscript{191} Tim Cook (@tim_cook), TWITTER (Oct. 24, 2018, 2:57 AM), https://twitter.com/tim_cook/status/1055035549512294401.

\textsuperscript{192} \textit{See} Kosseff, \textit{supra} note 37, at 171, 178 (describing the close relation between data protection and cybersecurity and noting that the CCPA, which is aimed at data protection, also implements cybersecurity obligations).

\textsuperscript{193} \textit{Id}.

policies across the US.\textsuperscript{195} Not only does the current framework of
fragmentary federal legislation coupled with meticulously crafted local
laws leave the consumer wildly unprotected, but it also creates undue
burdens upon companies attempting to remain compliant.\textsuperscript{196}

E. Consent: Legal Fiction or Untapped Potential?

The CCPA and the Intel Data Privacy Proposal, to be discussed
further in Part III, both follow opt-out models of consent, and as such,
diverge from the main goal of the GDPR and of this Note's solution: data
subjects' unbridled control over their own personal information.\textsuperscript{197} With
the FTC's authority over data privacy, stemming from the ability to
prevent unfair or deceptive business acts or practices,\textsuperscript{198} consumer
uncertainty must be alleviated through the adoption of the opt-in model of
consent.\textsuperscript{199} In their article, Transatlantic Data Privacy Law, Paul
Schwartz and Karl-Nikolaus Peifer comment that "[i]n the uncertain
privacy landscape of the United States, the FTC has stopped companies
from tricking consumers, overpromising privacy, and engaging in
unexpected and unreasonable data practices."\textsuperscript{200} However, the article calls
this "idealized consent" mere "legal fiction."\textsuperscript{201} The article goes on to
explain Lon Fuller's definition of legal fiction as the "reconciliation of a
'legal result with some expressed or assumed premise.'\textsuperscript{202} This is based
on the assumption that the imaginary reasonable consumer does take the
time to read privacy policies.\textsuperscript{203} Nevertheless, this is a dangerous
generalization to make as it fails to take into account the impact of
continuous privacy reminders in the aggregate, as well as undervalues the
benefits the FTC has to gain from a uniform notice-and-consent model.\textsuperscript{204}

The most common privacy notices today are unwieldy, overly
complicated with legalese, and focus more on statutory requirements
rather than informing the consumer.\textsuperscript{205} To promote consumer
understanding, the conversation must turn on whether corporations are

\textsuperscript{195} Id.
\textsuperscript{196} See id.
\textsuperscript{197} See infra Parts III, IV.
\textsuperscript{198} Schwartz & Peifer, supra note 49, at 149. The FTC currently operates in the realm of
privacy protection under the presumption that a reasonable data subject maintains certain privacy
policy expectations. Id. These expectations—being either explicitly or implicitly promised by ways
of industry norms—can be enforced under the FTC's authority to prevent unfair or deceptive acts
affecting commerce. Id.
\textsuperscript{199} See infra Part IV.
\textsuperscript{200} Schwartz & Peifer, supra note 49, at 150.
\textsuperscript{201} Id. at 149-50.
\textsuperscript{202} Id. (quoting LON L. FULLER, LEGAL FICTION 51 (1967)).
\textsuperscript{203} Schwartz & Peifer, supra note 49, at 150.
\textsuperscript{204} See id. at 148.
\textsuperscript{205} Florian Schaub et al., Designing Effective Privacy Notices and Controls, IEEE INTERNET
providing consumers with necessary decision-making information.\footnote{206} In order to create effective privacy notices, the three requirements of (1) relevancy, (2) actionability, and (3) understandability must be met.\footnote{207} A privacy notice is relevant if it provides a data subject with information pertaining to the current transactional context, so as to better understand the instant privacy implications.\footnote{208} Actionability is met when data subjects are given the ability to freely give or withhold consent based upon explicit expressions of choice rather than an assumption based on prior or aggregated user usage.\footnote{209} Understandability, a straight-forward concept, is lost in the privacy policies of today as they often bombard the data subject with an unnecessary amount of information.\footnote{210} Instead, it must be a priority to make privacy notices easily comprehensible to the non-lawyer.\footnote{211}

The current practice of presenting privacy policies in their entirety leads to "information overload" and is simply an ineffective way of informing data subjects.\footnote{212} Instead, privacy policies can be complemented with brief privacy notices, formed within the boundaries of relevancy, actionability, and understandability, and tailored to specific transactional contexts.\footnote{213} These privacy notices—remaining short and specific—would require a data subject to rely less on interpretation and focus more on creating informed decisions as to the boundaries and implications of his or her consent.\footnote{214}

\section*{III. Data Privacy: Who is Driving the Discussion?}

The need for constitutional data privacy rights that provide real protection on the Internet is becoming more and more apparent.\footnote{215} The "Internet pervades all aspects of life" and the current disorganized system of data privacy law will no longer cut it.\footnote{216} This Part examines Senator

\begin{itemize}
\item \footnote{206} See \textit{id.} at 73.
\item \footnote{207} \textit{Id.} at 72.
\item \footnote{208} \textit{Id.}
\item \footnote{209} \textit{Id.}
\item \footnote{210} \textit{Id.} at 72, 73.
\item \footnote{211} \textit{Id.} at 73.
\item \footnote{212} See \textit{id.} at 71, 73.
\item \footnote{213} \textit{Id.} at 72, 73.
\item \footnote{214} \textit{Id.} at 73.
\item \footnote{216} \textit{Id.} at 1107-08.
\end{itemize}
Wyden’s bill, Intel’s Proposal, and the CCPA in order to give examples of differing viewpoints on the best way forward—as well as highlight the fundamental issues with each approach.

Critics of a comprehensive federal data privacy framework argue overregulation would interfere with the development and innovation of domestic data markets. These concerns stem from the United States’ view that data privacy is a purely commercial endeavor, as the “processing of personal data constitutes quite a considerable part of the entire market sector.” Because of this fact, “[g]overnment actors do not want to kill the goose that lays the golden eggs,” and with that mentality, they trust private entities to self-regulate. However, after a year full of bipartisan backlash against Big Tech in 2018, the list of growing supporters for data privacy legislation has since grown steadily. In regard to this growing support, Neema Singh Guliani, senior legislative counsel at the American Civil Liberties Union, stated: “You have a bipartisan sense that some type of privacy legislation needs to happen, and at the same time, you have industry pushing for it.” The Legislature is not the only branch of government voicing concerns over data privacy and asking for guidance. On September 25, 2018, the Trump Administration’s National Telecommunications and Information Administration issued a request for comments and described a seven-point privacy protection outline for favorable outcomes. Subpart A of this Part analyzes Senator


220. See infra Parts III.A–C.


222. JOANNA KULESZA, INTERNATIONAL INTERNET LAW 58 (Magdalena Arent & Wojciech Woloszyk trans., 2012).

223. Watanabe, supra note 221, at 1124.

224. Lapowsky, supra note 187. The term “Big Tech” refers to “four or five major technology companies, namely Facebook, Apple, Google, and Amazon. Microsoft is occasionally added to the list,” Naveen Joshi, What Is Big Tech and Why Should We Care, ALLERIN (Aug. 21, 2019), https://www.allerin.com/blog/what-is-big-tech-and-why-we-should-care.

225. Lapowsky, supra note 187.

226. Id.

Wyden’s bill and its regulatory missteps.\textsuperscript{228} Subpart B examines Intel’s unique take on the legislative balancing required to regain public trust and promote innovation.\textsuperscript{229} Subpart C looks toward the nation’s leading example in comprehensive data privacy legislation—California.\textsuperscript{230}

A. The GDPR Has Teeth and Wyden’s Bill Has Fangs

"There need[s] to be consequences when corporations don’t protect your data” claimed Ron Wyden, Democratic senator from Oregon, “[m]y bill will put reckless CEOs in jail if they lie about protecting your personal information.”\textsuperscript{231} Wyden took to Twitter after releasing his discussion draft labeled “Consumer Data Protection Act,”\textsuperscript{232} in hopes of gaining public support in delegating direct enforcement authority to the FTC under the Federal Trade Commission Act.\textsuperscript{233} Having incorporated comments and feedback following the discussion draft, Wyden’s next bill, introduced to Congress as “Mind Your Own Business Act of 2019,” calls for increased transparency on how corporations sell, share, and use personal data.\textsuperscript{234} In similar fashion to the GDPR, the bill provides for steep penalties for not only the corporation itself, but also for executives in light of personal data breaches.\textsuperscript{235} According to one writer, “if [the] GDPR has teeth, Wyden’s proposal has fangs—set on the jugulars of corporate heads[,]”\textsuperscript{236} it focuses less on individuals’ rights and more on expanding the FTC’s authority to regulate data privacy, and the bill also takes after the GDPR in its ability to fine a corporation up to four percent of global, annual revenue.\textsuperscript{237} Yet, the bill takes penalties a step further, as it also subjects executives to up to twenty years of jail time and to fines reaching $5 million per infraction
for CEOs who knowingly lie or mislead privacy regulators.\textsuperscript{238} This is great to hold those that mishandle an individual’s personal information accountable, but what else does it do to alleviate consumer concern over whether her privacy interests are being adequately respected?\textsuperscript{239} Acknowledging that holding executives accountable for their actions is most certainly beneficial,\textsuperscript{240} appropriate legislation must still afford consumers more proactive means of protection.\textsuperscript{241} One main difference that distinguishes the Wyden bill from the GDPR, Intel proposal, and CCPA,\textsuperscript{242} is the presence of a national “do not track” list for consumers.\textsuperscript{243} This “do not track list” would allow American data subjects to preemptively opt-out within their web browser settings to data sharing, selling, or ad-targeting based on personal information.\textsuperscript{244} Calling for more individual freedom and control is the purpose of this Note, but this “do not track” list is hardly the solution needed.\textsuperscript{245} The proposal “protects” privacy only by making it a violation to deny services to those exercising this right.\textsuperscript{246} In order to effectuate this, Wyden’s bill further permits covered entities to create a paid-for version of the application in order to offset losses incurred.\textsuperscript{247} These paid-for versions would best resemble subscription ad-free models, the costs of which would be capped in relation to what the entity would have gleaned from sharing user data.\textsuperscript{248} The bill, tasking the FTC with the creation of the national “do not track”

\begin{footnotes}
\item[238] S. 2637 § 5(d)(2); see Hackett, \textit{supra} note 235.
\item[241] \textit{See supra} text accompanying notes 188-91.
\item[242] \textit{See infra} text accompanying notes 244-53.
\item[243] S. 2637 § 6; \textit{Wyden Press Release, supra} note 239.
\item[245] \textit{See infra} text accompanying notes 322-25.
\item[247] S. 2637 § 6(b)(2); Amerding, \textit{supra} note 244; \textit{Wyden Press Release, supra} note 239.
\item[248] S. 2637 § 6(b)(2)(B); Davis, \textit{supra} note 246; see Amerding, \textit{supra} note 244; \textit{Wyden Press Release, supra} note 239 ("The bill ensures that privacy does not become a luxury good by requiring companies to offer privacy-protecting versions of their products for free to consumers who are eligible for the FCC’s Lifeline program.").
\end{footnotes}
list, completely misses the mark on giving the power back to the consumers.249

Wyden’s bill follows the same ineffective opt-out model currently in use.250 Instead of following the GDPR’s lead in giving the control back to data subjects via opt-in social contracts, the Wyden bill sticks with the same faulty FTC endorsed system that has yet to yield any success since the original “do not track” list was improperly implemented in 2010.251 The proposed variation not only fails to take into consideration the necessity of rebuilding the trust between those tech companies that have misused personal data and the public, but it also fails to consider the power of individualized transactions.252

Given that the Wyden bill focuses on a “one-stop shop” opt-out method, Wyden’s bill in effect takes all decision-making power away from the individual, while masquerading the option as a consumer necessity.253 By only providing a single “opt-out of all data practices” option, the bill prevents the individual from making an informed decision about any subsequent data transaction or web usage.254 Instead of this faulty model, consent needs to revolve around a “continuous process of reassessment, ensuring data practices are reasonable and transparent, ultimately establishing and maintaining fair terms of business.”255 In commenting on Wyden’s discussion draft, Marco Rubio, a Republican Senator from Florida, told reporters that he believes “most Americans view their online behavior as personal property.”256 Without allowing individuals the opportunity to decide consent transaction-to-transaction, the Wyden bill fails to give the adequate level of consumer control this Note calls for.257

Wyden’s bill, with its guillotine-style enforcement mechanisms against corporations and their CEOs, falls short of becoming the sweeping


250. Id.

251. Davis, supra note 246.

252. See Chad Wollen, Opt In, Opt Out — Consent Is What It’s All About, IAPP (Oct. 31, 2018), https://iapp.org/news/a/opt-in-opt-out-consent-is-what-its-all-about (stating that consent mechanisms which revolve around continuous reassessment are more likely to engender more trust moving forward).

253. See Dell Cameron, Wyden Unveils Plan to Protect Private Data, Restore ‘Do Not Track,’ and Jail Reckless CEOs, GIZMODO (Nov. 1, 2018, 11:48 AM), https://gizmodo.com/wyden-unveils-new-plan-to-protect-private-data-restore-1830153516; Wollen, supra note 252 (arguing that consumer consent should not be a “one-off event”).

254. See generally Wollen, supra note 252 (explaining the importance of a transparent individualized transaction-based consent regime).

255. Id.

256. Laslo, supra note 249.

257. See infra text accompanying notes 356-59.
standard for data protection.\textsuperscript{258} The reason for this is because the bill would not preempt any state privacy laws.\textsuperscript{259} Generally speaking, it would fail to alleviate the complications caused by the patchwork of sectoral, federal, and state laws.\textsuperscript{260} In order to best promote consistency and understanding of the law in the developing field of data privacy, the adoption of a single comprehensive data privacy law can be the only solution—\textsuperscript{261}the vision of which is in line with both the Chamber of Commerce\textsuperscript{262} and the Internet Association.\textsuperscript{263} With the current haphazard system of privacy protection, a bill that does not preempt state laws concerning data privacy results in uncertainty and inconsistency for both consumers and businesses.\textsuperscript{264} All things considered, consumers and businesses “lose when they have to navigate a confusing and inconsistent patchwork of state laws,”\textsuperscript{265} and this is further evidence as to why the Wyden bill is not a viable option.\textsuperscript{266}

\section*{B. A Tech Giant’s Swing at Data Privacy}

According to David Hoffman, Intel’s Associate General Counsel and Global Privacy Officer, “The collection of personal information is a growing concern. The US needs a privacy law that both protects consumer privacy and creates a framework in which important new industries can prosper.”\textsuperscript{267} Hoffman further explained that Intel’s proposal is “designed to spur discussion that helps inspire meaningful privacy legislation.”\textsuperscript{268} The heart of Intel’s proposal, which is sure to be “the most controversial part of any coming legislation,” is the consequences associated with

\begin{itemize}
  \item \textsuperscript{258} See Dan Clark, US Senator Proposes Data Protection Bill Imposing Criminal Fines and Penalties for Breaches, LAW.COM (Nov. 7, 2018, 4:12 PM), https://www.law.com/corpconseul2018
  \item \textsuperscript{261} "See supra text accompanying notes 258-65.
  \item \textsuperscript{262} Id.; see David Hoffman & Riccardo Masucci, Intel’s AI Privacy Policy White Paper, INTEL 2 (Oct. 22, 2018), https://blogs.intel.com/policy/files/2018/10/Intels-AI-Privacy-Policy-White-Paper-2018.pdf. Intel’s paper, while specifically directed towards privacy risks associated with automated data collection, remains in line with this Note’s solution as it calls for comprehensive, technologically neutral legislation that supports the free flow of data. Id.
\end{itemize}
noncompliance.\textsuperscript{269} Unlike Wyden’s bill, the Intel proposal would allow the FTC to impose criminal fines up to one million dollars, a cap on executive imprisonment to not exceed ten years, and civil penalties of no more than one billion dollars for noncompliance.\textsuperscript{270} Intel’s proposal forces covered entities’ executives into the limelight when they misuse personal data, but it surprisingly does not require notification to data subjects when a breach takes place.\textsuperscript{271}

In fact, Intel’s privacy bill does nothing to address what happens in the event of a data breach.\textsuperscript{272} For comparison purposes, the typical state law regarding data privacy requires notification to data subjects following a data breach within thirty to sixty days.\textsuperscript{273} Not only does Intel’s proposal substantially deviate from the model used at the state level, but it also pales in the light of the seventy-two hour notification requirement set forth by the GDPR.\textsuperscript{274} Understanding the current atmosphere around personal data privacy and reasonable consumer expectations thereof, “it would appear that the Intel privacy bill still falls short of what is now considered best practices in the data privacy world.”\textsuperscript{275} According to the Privacy Rights Clearinghouse, an institution maintaining a chronology of data breaches, there have been almost ten thousand data breaches publicly recorded since 2005.\textsuperscript{276} Further shedding light onto this epidemic, under state-level privacy regimes, most industries are not required to provide detailed information surrounding the circumstances of a breach.\textsuperscript{277} The sheer lack of transparency is the reason why companies hands’ have not been forced to act sooner: “Most companies in this country still have not embraced a corporate culture where privacy and security are core values.”\textsuperscript{278} Most industries simply decide to leave people in the dark as they are not required to give detailed notifications following a data breach.


\textsuperscript{270} \textit{Compare Innovative and Ethical Data Use Act of 2019}, supra note 218, §§ 6(b)(1)(B), (2)(C) (capping criminal fines at one million dollars with ten years imprisonment and civil fines at one billion dollars), \textit{with Inside Privacy}, supra note 239 (explaining that Wyden’s privacy proposal carries criminal penalties of up to five million dollars and twenty years imprisonment, as well as civil penalties of up to $50,000 per violation or four percent total annual gross revenue).

\textsuperscript{271} Clark, supra note 267.


\textsuperscript{273} \textit{Id.}

\textsuperscript{274} GDPR, supra note 4, at art. 33; Lindsey, supra note 272.

\textsuperscript{275} Lindsey, supra note 272.


\textsuperscript{278} See id.
breach. Without the necessary precautions and proper notification of compromised data, consumers cannot effectively protect themselves.

The Intel proposal follows the same opt-out model of consent as Wyden’s bill, except that certain data, deemed to be of “high risk,” would require explicit pre-collection consent. Wanting to get ahead of the push for federal legislation, Intel’s purpose for this proposal is to balance consumers’ privacy rights against a framework conducive to tech industry growth. The “risk-based accountability” holds companies to a higher standard when data that “is likely to create significant privacy risk” is collected and provides consumers with the strongest safeguards for this category of information. Covered entities seeking to collect and process such sensitive information will be required to give explicit notice and gain pre-collection consent. It should come as no surprise that the proposal from an actor within the tech industry would choose the ineffective opt-out method of data collection. Opt-out regimes are notorious for limited opt-out mechanisms that are both difficult to exercise and intentionally broad, vague, and hidden. It would also be incorrect to believe it is even feasible to categorize sensitive high-risk information separately from non-sensitive. This concept is flawed as it fails to take into account the fluidity of data and its ability to change: “The interconnectedness of data and data processors can quickly turn non-sensitive data into ‘sensitive’ data.”

C. California: The Leading State in Data Protection

The CCPA, officially titled AB-375, was signed by the state governor on June 28, 2018 and is one of the strictest privacy laws seen

279. Id.
280. Id.
281. Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(f)(2) (classifying significant privacy risk data to include: (1) geolocation data; (2) biometric data; (3) racial or ethnic data; (4) religious practices data; (5) “physical and mental health data, including any past or present information regarding an individual’s medical history, mental or physical condition, medical treatment, or diagnosis by a health care professional”; (6) “sexual life” data, “including sexual activity, sexual orientation, sexual preference and/or sexual behavior”; (7) genetic data; and (8) activities where the data subject has a reasonable expectation of privacy).
282. Lindsey, supra note 272.
283. Id.
284. Innovative and Ethical Data Use Act of 2018, supra note 218, § 4(g)(7).
285. Lindsey, supra note 272.
287. See Lindsey, supra note 272.
288. Tomain, supra note 2, at 2.
289. Id. at 31.
290. Id.
291. Id.
in the United States.\textsuperscript{293} The CCPA, which went into effect January 1, 2020, brought with it data privacy protections and controller/processor requirements similar to those seen in the GDPR.\textsuperscript{294} It is noteworthy to mention that the backdrop for this data privacy statute is similar to that in the EU for the GDPR.\textsuperscript{295} Just as the EU sees data privacy to be a fundamental right, so too does California see privacy to be an inalienable right of the people.\textsuperscript{296} In 1972, California added “privacy” to the list of inalienable rights in Article 1, Section 1, of the California Constitution.\textsuperscript{297} It is clear after observing the legislative history of California’s privacy clause that the privacy clause was intended to be a stand-alone right, not to be limited by other rights.\textsuperscript{298}

With some of the most robust data privacy laws in the nation,\textsuperscript{299} California privacy law applies to all persons and businesses in California that own or license personal information.\textsuperscript{300} Enshrined within the legislation is the intent of the Legislature and the goal of the CCPA is to provide Californians with the following rights:

(1) [t]he right of Californians to know what personal information is being collected about them[;] (2) [t]he right of Californians to know whether their personal information is sold or disclosed and to whom[;] (3) [t]he right of Californians to say no to the sale of personal information[;] (4) [t]he right of Californians to access their personal information[;] and] (5) [t]he right of Californians to equal service and price, even if they exercise their privacy rights.\textsuperscript{301}

The penalties for breach or noncompliance pale in comparison to that of the GDPR, the Wyden bill, or even Intel’s proposal.\textsuperscript{302} The CCPA’s

\textsuperscript{293} California Passes Nation’s Strictest Data Privacy Law, DUANE MORRIS (July 9, 2018), https://www.duanemorris.com/alerts/california_passes_nations_strictest_data_privacy_law_0718.html; Nicastro, supra note 292 (discussing the various obligations imposed by the CCPA).

\textsuperscript{294} Compare CAL. CONST. art. 1, § 1 (identifying privacy as an inalienable right), with Charter of the Fundamental Rights of the European Union, art. 8, Oct. 26, 2012, 2012 O.J. (C 364) 391 (dictating that data subjects have the explicit right to data and informational privacy).

\textsuperscript{295} CAL. CONST. art. 1, § 1 (amended 1972).

\textsuperscript{296} J. Clark Kelso, California’s Constitutional Right to Privacy, 19 PEPP. L. REV. 327, 433 (1992) (“The committee reports indicate that the Legislature was well aware of the limited extent of the federal right to privacy and that the federal right to privacy existed only by virtue of penumbral emanations from other provisions in the Bill of Rights.”).


\textsuperscript{298} AB-375 Privacy: Personal Information: Businesses, CAL. LEGIS. INFO. (June 29, 2018, 4:00 AM), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

\textsuperscript{299} Compare CAL. CIV. CODE. § 1798.150(a)(1)(A) (West 2018) (capping private causes of action at $750 per violation or actual damages), and CAL. CIV. CODE. §§ 1798.155(a)–(b) (2018) (capping state civil actions at $7500 per intentional violation if not cured within thirty days), with GDPR, supra note 4, at art. 83(5) (permitting an administrative fine up to four percent of global,
private cause of action—stemming from breach or unauthorized access of personal information—permits consumers to seek statutory damages up to $750 per incident or actual damages, whichever is greater.\textsuperscript{303} To be covered under the CCPA, an entity would need to meet one of the following thresholds: (1) have a gross annual revenue of at least $25 million, (2) commoditize the personal information of at least 50,000 individuals, or (3) derive at least fifty percent of its annual revenues from personal information commoditization.\textsuperscript{304} Despite privacy being an explicit right within California’s Constitution,\textsuperscript{305} the scope of the CCPA seems to be set to a different standard.\textsuperscript{306} Whereas the GDPR’s scope encompasses data processors and controllers of EU citizens’ data irrespective of size,\textsuperscript{307} the CCPA’s scope is limited to for-profit businesses in California having also met the previously mentioned classifications.\textsuperscript{308} When the right to privacy of both the CCPA and GDPR is founded based on California’s Constitution\textsuperscript{309} and the Charter of Fundamental Rights of the European Union,\textsuperscript{310} respectively, why is it that the scope and territorial reach of the CCPA are drastically undersized in comparison?\textsuperscript{311} Of course, the wide net that the GDPR casts can have negative consequences on small businesses,\textsuperscript{312} but this Note posits that a greater danger is having a law that permits smaller entities to completely disregard codified privacy interests.\textsuperscript{313}

Deviating substantially from the approach taken in Wyden’s bill,\textsuperscript{314} the CCPA brings with it a number of individual rights\textsuperscript{315} and the nation’s annual revenue), Mind Your Own Business Act of 2019, S. 2637, 116th Cong. § 5(d)(2) (2019) (providing criminal penalties up to five million dollars and twenty years imprisonment), and Innovative and Ethical Data Use Act of 2019, supra note 218, § 6(b)(1)(B) (stipulating criminal fines may reach one million dollars or ten years imprisonment and civil penalties arising from the same acts or incident capped at one billion dollars).

303. § 1798.150(a)(1)(A).
304. §§ 1798.140(c)(1)(A)–(C).
305. CAL. CONST. art. 1, § 1.
307. GDPR, supra note 4, at art. 3. But see GDPR, supra note 4, at art. 30(5) (limiting record keeping obligations for controllers and processors of less than 250 employees).
308. § 1798.140(e)(1).
309. CAL. CONST. art. 1, § 1.
311. See Jehl & Friel, supra note 306, at 1.
313. See generally Part II.D.1 (clarifying the goal of protecting data subjects’ privacy interests, irrespective of entity size).
315. CAL. CIV. CODE. §§ 1798.100–125 (West 2018). The CCPA provides California data subjects the right to (1) know whether personal information is being collected, (2) know what
first statutory opt-in requirement for information relating to minors under the age of sixteen.\textsuperscript{316} Be that as it may, the opt-in provision of the CCPA is only applicable to the sale of personal information.\textsuperscript{317} Generally speaking, under the CCPA, covered entities are permitted to process personal information without pre-collection consent (unless the consumer is under sixteen and the sale of which is the purpose for processing).\textsuperscript{318} Operating under an ineffective right-to-know, the CCPA only requires disclosure as to the categories of data—but when it comes to individual autonomy, affirmative consent is the necessary golden standard.\textsuperscript{319} Notwithstanding the failure to carve out a narrower exception,\textsuperscript{320} the California legislature has successfully created an initial framework for a rights-based data privacy law necessary for our data-driven world.\textsuperscript{321}

IV. THE NECESSARY STATUTORY GUIDANCE IN DATA PRIVACY LAW

The booming marketplace of data commoditization raises serious privacy concerns, often without consumer awareness of the threat presented.\textsuperscript{322} The public needs assurance that personal information, whether shared knowingly or unknowingly, is being appropriately protected.\textsuperscript{323} To best protect American data subjects in today’s data-centric world, a single comprehensive federal legislative initiative must come into fruition.\textsuperscript{324} To this end, Part IV examines the necessary building blocks of a federal data privacy regime and introduces the language best equipped to achieve individualized rights.\textsuperscript{325}

In order to achieve such legislative goals, a few things must be realized: (1) a national standard for determining covered entity status,\textsuperscript{326} (2) limitations on the collection and processing of personal information,\textsuperscript{327}

---

\textsuperscript{316} California Passes Nation’s Strictest Data Privacy Law, supra note 293.
\textsuperscript{317} § 1798.120(c)-(d).
\textsuperscript{318} Jehl & Friel, supra note 306, at 1.
\textsuperscript{320} § 1798.140(c).
\textsuperscript{321} §§ 1798.100-125.
\textsuperscript{323} Id.
\textsuperscript{324} See id.
\textsuperscript{325} See infra text accompanying notes 331-59, 369-76. 
\textsuperscript{326} See infra text accompanying notes 331-37.
\textsuperscript{327} See infra text accompanying notes 338-40.
(3) security by design framework, 328 and (4) a mandatory distinction between privacy policies and privacy notices—coupled with affirmative consent. 329 A statutory framework, similar to that provided below, would give data subjects the tools essential to protect the pseudo-property interests in their personal data. 330

1. Implementation of Fair Information Practice Principles.

(A) Covered Entity 331 – Any legal person over which the FTC has authority pursuant to: (i) Section 5(a)(2) of the Federal Trade Commission Act, 332 (ii) common carriers subject to FTC authority under the Communications Act of 1934, 333 notwithstanding Section 5(a)(2) as described herein; (iii) any organization related to a covered entity by means of common ownership or corporate control; and (iv) third parties not related to a controller as defined by Section 1(A)(iii) but which process at the direction and as an instrumentality of said controller, 335 notwithstanding Section 5(a)(2) as described herein. 336 Exception – In order to accommodate the needs and capabilities of small to medium sized entities, the FTC shall be empowered to enact Rules regarding entities controlling personal data of less than 5000 data subjects and that derive less than fifty percent of its total annual revenue through the commoditization of personal data. 337

(B) Collection Limitation – All data collection done by covered entities shall not exceed that which is relevant and necessary in order to accomplish a specified purpose as laid out in Section 1(E) 338 and in accordance with Section 1(I) herein. 339

328. See infra text accompanying notes 344–48.
330. See infra text accompanying notes 331–59, 369–76.
331. See Innovative and Ethical Data Use Act of 2019, supra note 218, § 3(c) for a domestic definition of covered entity. Intel’s approach to covered entity status has been adopted for purposes of this Note. See also CAL. CIT. CODE §§ 1798.140(c)(1)(A)–(C) (West 2018) (conferring covered entity status when one of the following thresholds is met: (1) gross revenues in excess of twenty-five million dollars, (2) oversees personal information of 50,000 data subjects, or (3) fifty percent of annual revenue derives from such data commoditization); GDPR, supra note 4, at arts. 3(1)–(3) (defining the GDPR’s broad territorial scope to encompass the processing of personal data in connection to controllers and processors within the EU, those entities offering goods or services within the EU, or the monitoring of data subjects’ behavior within the EU).
335. See Innovative and Ethical Data Use Act of 2019, supra note 218, § 3(m).
337. See CAL. CIT. CODE § 1798.140(c) (West 2018). This language is consistent with the general theme of the CCPA and Intel proposal in that room is left open for how to best alleviate pressures of this Act on small to medium sized entities. Id.; see also Innovative and Ethical Data Use Act of 2019, supra note 218, § 3(c)(4). But see GDPR, supra note 4, at art. 3(1)(3).
338. See GDPR, supra note 4, at art. 5(1)(c) (defining a comparable data minimization limitation); Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(a).
(C) Use Limitation – Covered entities shall be permitted to process personal information: (i) for purposes to which the individual has provided explicit consent to processing, unless otherwise prohibited by law, regulation, or public policy; or (ii) as a requirement of law or regulation, including request by governmental agency. 340

(D) Data Quality – Covered entities, to the extent reasonable for purposes of processing personal data, shall maintain complete, accurate, and up to date records of personal information as required to maintain accuracy. 341

(E) Purpose Specification – Covered entities shall provide notices required by Section 1(H) describing collection purposes, including both general and direct notices, made in clear language explicitly stating intended data use purposes. 342 (i) Time of Specification – The Purpose of collection must be specified no later than the time of collection unless otherwise impossible or impracticable. 343

(F) Security Safeguards – Covered entities shall develop, document, implement, and maintain, whilst taking into account costs of implementation with the likelihood of integrity failure, appropriate technical and organizational measures to ensure appropriate levels of data security: 344 (i) pseudonymization and encryption of personal data; 345 (ii) ability to ensure the ongoing security, integrity, confidentiality, and availability of personal data; 346 (iii) regular testing, assessing, and evaluating of technical and organizational security measures and the effectiveness thereof; 347 (iv) comply with security measures and procedures set forth in Section 1(G). 348

(G) Notification of Personal Data Breach 349 – In the event of a personal data breach: (i) the controller is to report, upon knowledge of the breach, to the FTC without undue delay; 350 (ii) the processor shall notify the controller upon knowledge of the breach without undue delay relevant information surrounding the breach; 351 (iii) the controller shall, upon

340. See GDPR, supra note 4, at arts. 5(1)(b)–(c) (defining a comparable purpose limitation); Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(d).
341. See GDPR, supra note 4, at art. 5(1)(d) (defining a comparable accuracy requirement); Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(b).
342. GDPR, supra note 4, at art. 5(1)(c); Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(c).
344. GDPR, supra note 4, at art. 32(1).
345. Id. at art. 32(1)(a).
346. Id. at art. 32(1)(b).
347. Id. at art. 32(1)(d).
348. See infra text accompanying notes 349-52.
349. GDPR, supra note 4, at arts. 33–34. This language, modeled after the GDPR and promoted herein, is necessary to strengthen trust in the Internet and allow data subjects material information in light of a data breach. Id.
350. GDPR, supra note 4, at art. 33(1).
351. Id. at art. 33(2).
knowledge of the breach, communicate without undue delay to affected data subjects.\footnote{352}{Id. at art. 34(1). The language of undue delay and its corresponding limitation of being no later than seventy-two hours after becoming aware is adopted herein. \textit{Id.} at art. 34(1).}

(H) Openness – A covered entity shall provide individuals and governmental agencies with information concerning its personal data practices.\footnote{353}{Innovative and Ethical Data Use Act of 2019, supra note 218, § 3(f)(1).} (i) General Notice – A covered entity shall provide data subjects with relevant, actionable, and understandable privacy information alongside the action for consent set forth in Section 1(I),\footnote{354}{\textit{Id.} § 3(f)(3).} and (ii) Complete Notice – A covered entity shall publish and make publicly readily available, to be updated on an ongoing regular basis, full and complete description as to the specifics of personal information collected and privacy practices used.\footnote{355}{\textit{Id.} § 3(f)(4).}

(I) Consent – Covered entities are required to receive a clear and unambiguous affirmative consent to specific data collection.\footnote{356}{GDPR, supra note 4, at rec. 32; \textit{Contra Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(f)(2)} (choosing the opt-out model of consent for data not otherwise captured by the risk-based analysis).} Such consent is to be provided in clear and plain language, to be distinguishable from consent of other matters.\footnote{357}{\textit{Id.} at art. 7(2).} At any time, a data subject may make clear to a covered entity, to which consent has been previously provided to, of objection to further collection and present process of personal data.\footnote{358}{\textit{Id.} at art. 21(1).} This right to opt-out shall be provided in clear and unambiguous language in readily accessible locations, whether by internet or physical copy.\footnote{359}{See id.}

Section 1(H) is of great importance to this Note’s rejection of the notion that “idealized consent” is but legal fiction.\footnote{360}{See supra text accompanying notes 353-55.} Privacy policies, while generally considered essential aspects of data privacy, "are surprisingly ineffective at informing users or allowing them to express choice."\footnote{361}{Schaub et al., supra note 205, at 70.} This Note sets out to solve this exact difficulty.\footnote{362}{See supra text accompanying notes 353-55.} Sections 1(H)(i) and 1(H)(ii) of the proposed statute make the distinction between a general notice, giving consumers readily available and easily digestible information, and a complete notice, a reasonably full and complete description of a covered entity’s data practices, the form of which most privacy policies today adhere to.\footnote{363}{See supra text accompanying notes 353-55.} The distinction to be made is a fine line drawn between privacy policies, which are intended for regulators and legal experts in order to showcase compliance, and privacy notices,
which are designed for users in an auxiliary fashion to compliment the privacy policies.364

Section 2 of the proposed statute addresses data subject rights, mirroring those provided for in the GDPR365 and drafted in language suitable for constitutional permissibility based on language found in the CCPA366 and Intel’s proposal.367 The following provisions are necessary because, above all else, data subjects’ rights must be safeguarded.368

2. Data Subject Rights – Covered entities are to maintain systematic and organizational structures to ensure the following rights of its data subjects are properly observed:

(A) Right to Know – Privacy notices outlined in Section 1(H)369 shall contain the following information before consent of Section 1(I)370 is to be deemed fully informed: (i) whether personal information of the data subject is being or will be processed by the covered entity,371 (ii) description as to the nature and category of such personal information;372 (iii) plain language explanations of the covered entity’s data processing practices, including practices of processors or third parties otherwise included within Section 1(A) of this act;373 and (iv) descriptions of all rights contained within Section 2 of this act.374

(B) Right to Access – Covered entities are to provide a data subject, upon request and without undue delay, with the personal information of the data subject being processed in a commonly used electronic form.375

(C) Right to Equal Services – American data subjects have the right to equal service and price, even if they exercise one of the previous privacy rights enumerated herein.376

364. See Schaub et al., supra note 205, at 72, 73.
365. GDPR, supra note 4, at arts. 12–23.
367. Innovative and Ethical Data Use Act of 2019, supra note 218, § 3(g).
368. See infra text accompanying notes 369-76.
369. See supra text accompanying notes 353-55.
370. See supra text accompanying notes 356-59.
371. GDPR, supra note 4, at arts. 13(1), 14(1); California Consumer Privacy Act of 2018, SULLIVAN & CROMWELL LLP 3 (July 2, 2018), https://www.sullcom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf (explaining the right to know as outlined in the CCPA); Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(g).
372. GDPR, supra note 4, at arts. 13(1), 14(1); California Consumer Privacy Act of 2018, supra note 371, at 3; Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(g).
373. GDPR, supra note 4, at arts. 13(1), 14(1); California Consumer Privacy Act of 2018, supra note 371, at 3; Innovative and Ethical Data Use Act of 2019, supra note 218, at 13.
374. See supra text accompanying notes 369-76.
375. GDPR, supra note 4, at art. 15; California Consumer Privacy Act of 2018, supra note 371, at 4; Innovative and Ethical Data Use Act of 2019, supra note 218, § 4(g)(5).
376. CAL. CIV. CODE. § 1798.125(a)(1) (West 2018). A business is permitted to charge a consumer a different rate so long as the difference is "reasonably related to the value provided to the business by the consumer’s data." Id. § 1798.125(a)(2).
This Act works to strike the proper balance between consumer control and an environment conducive to tech innovation. Data processors and controllers have gone largely unchecked—their practices remain opaque and void of meaningful consumer choice. It cannot be overstated that "with the emergence of new sources of information, improvements in analytic methods, and the availability of more granular information about individual consumers, the need for consumer protections in this area has never been greater."

V. CONCLUSION

It is evident through the rapid expansion of the digital environment, public misunderstanding of data collection and processing practices, and distrust in the current self-regulated regime that an all-encompassing data protection law must be enacted. The public acceptance of the GDPR throughout the EU can be used to show the international concern over data protection and a willingness to work toward a uniform system. It is wholly impossible to understand privacy independent of society: "The need for privacy is a socially created need," sociologist Barrington Moore observed. The need for privacy is born out of societal conflict and the friction between actors; privacy is the relief that allows individuals to interact in ways otherwise difficult or impractical. The Internet is no longer a luxury, but a necessity; nearly all American data subjects with means to access the Internet have done so and U.S. legislation has been slow to catch up to the evolving societal privacy expectations. California, as the leader in data privacy law, gives Congress the most significant indicator of the need for legislation: that privacy itself is an inalienable right and the time has come for data privacy to be treated as

377. See infra text accompanying notes 331-59, 369-76.
378. FED. TRADE COMM'N, supra note 85, at i, 57.
379. Id. at 57.
380. See Shields, supra note 176.
381. See Baraniuk, supra note 187 (arguing that in a fully functioning digital democracy a corporation should be required to ask the consumer for their data, not the other way around).
382. Solove, supra note 14, at 484.
383. Id.
385. CAL. CONST. art. 1, § 1.
such. It is time for data privacy legislation to come into force before more individuals fall victim to self-regulated shortcomings.

Aaron Shubert*